AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* (1) one Lenovo Yoga Laptop Computer; (2) one Samsung Galaxy S9+ cellular telephone; and (3) sixteen skimming devices	)	Case No. 18-mj-1185

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York *(identify the person or describe property to be searched and give its location)*: (1) one Lenovo Yoga Laptop Computer; (2) one Samsung Galaxy S9+ cellular telephone; and (3) sixteen skimming devices, which are more fully described in Attachment A which is attached hereto and incorporated by reference herein.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: Evidence pertaining to violations of Title 18, U.S.C. §§ 1029(a)(1), 1029(a)(4), and 1344, as more fully set forth in Attachment B which is attached hereto and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 1029(a) and 1344, and the application is based on these facts: SEE AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael L. Hamilton, Special Agent, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/23/18

Judge's signature

City and state: Buffalo, New York

JEREMIAH J. MCCARTHY, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michael L. Hamilton, being duly sworn, depose and state:

1. I have been employed as a Special Agent with the United States Secret Service (USSS) since 2017. The USSS is an agency within the Department of Homeland Security (DHS), which is a department within the executive branch of the United States Government. I have received formal training in the investigation of crimes involving Bank Fraud and Access Device Fraud. I have also received training from the Federal Law Enforcement Training Center, Glynco Georgia and the United States Secret Service, Beltsville, Maryland. Prior to my employment with USSS, I served for over seven years in the Department of Defense as an Army Officer, where I worked multiple intelligence-based investigations involving crimes against national security.

2. I make this affidavit in support of an application for warrants to search the following three items of electronic equipment all currently located in the Western District of New York (hereinafter referred to as "SUBJECT PROPERTY"): (1) one Lenovo Yoga Laptop Computer; (2) one Samsung Galaxy S9+ cellular telephone; and (3) sixteen skimming devices; all of which are more fully described in **Attachment A**.

3. The statements made in this affidavit are based upon my involvement in this investigation, as well as information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is

being submitted for the limited purpose of seeking a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 1029(a)(1) (production, use, or trafficking in one or more counterfeit access devices); 1029(a)(4) (production, trafficking, or possession of device-making equipment); and 1344 (bank fraud) exists on the SUBJECT PROPERTY.

I. STATUTORY DEFINITIONS

4. Pursuant to Title 18, United States Code, Section 1029(e)(1), the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

5. Pursuant to Title 18, United States Code, Section 1029(e)(2), the term "counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device.

6. Pursuant to Title 18, United States Code, Section 1029(e)(6), the term "device-making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device.

II. THE INVESTIGATION AND FACTUAL BASIS

7. On or about October 10, 2018, at approximately 8:03 p.m., JORGE ALBERTO-ALVAREZ ("ALVAREZ") attempted to enter the United States at the Peace Bridge Port of Entry, located in Buffalo, NY. During a primary inspection by Customs and Border Patrol (CBP) Officer Kanfeser, ALVAREZ stated that he had visited family in Detroit, Michigan, and that he was planning to drive back to Chicago, Illinois so that he could fly back to Miami, Florida. Based on inconsistencies in ALVAREZ's stated travel itinerary, Officer Kandefer initiated a trunk inspection. During the inspection, Officer Kandefer observed a suitcase, and in the suitcase was a small box containing a large quantity of various credit, debit, and bank cards bearing names other than ALVAREZ. As a result, ALVAREZ was sent for a secondary inspection and a further search of his vehicle.

8. During secondary inspection, CBP Officer Tabone asked ALVAREZ about his purpose for travel. ALVAREZ stated that he was on a mini vacation, that he traveled by air from Miami to Chicago, and then rented a car and drove to Michigan to attempt to meet up with a woman he had been communicating with on Facebook.

9. During the search of ALVAREZ's vehicle, Officer Tabone searched a black backpack in the backseat of the vehicle and discovered various gas station security seals, a Bluetooth magnetic card reader, a Lenovo Yoga Laptop Computer, and a Samsung Galaxy S9+ cellular telephone. During a search of the suitcase in the trunk of the vehicle, CBP Officer LaRosa located sixteen skimming devices, which are electronic communication devises consistent with those used in ATM skimming schemes. Additionally found was a small tool

kit containing a battery-operated drill, various drill bits, Allen wrench sets, and pry bars. Inside the small box in the suitcase was discovered a total of 90 credit and debit cards. Using a credit card reader, CBP determined that all of the cards appeared to have various names and account information encoded on them, and on the reverse side of the card, a four digit number was written in black marker. A subsequent patdown of ALVAREZ revealed 11 bankcards in his wallet, with 2 of the cards having various names and account information encoded on them. Additionally located in ALVAREZ's wallet was a New Jersey driver's license in the name of another individual but containing the photograph of ALVAREZ. Your affiant has determined that this New Jersey driver's license is counterfeit.

10. At approximately 1:02 a.m. on October 11, 2018, Special Agent Colafranceschi with Homeland Security Investigations (HSI) interviewed ALVAREZ in the presence of CBP officers. During the interview, ALVAREZ stated that he attempted to meet up with a friend in Michigan, but after being unable to find her, he decided to enter Canada to visit Niagara Falls, Ontario. When questioned about the items located in his vehicle, ALVAREZ stated he found the items next to a garbage pile in Miami, Florida. ALVAREZ admitted that he knew the cards were fraudulent and that he tried to use 3 of them at a gas station but was declined. ALVAREZ stated he used one of the names on the fraudulent cards to obtain a fraudulent New Jersey driver's license via the internet. ALVAREZ claimed that his friend in Michigan was going to buy all of the items that were found in his car for $4,000, and that was the reason for his travel.

11. At approximately 3:30 a.m., your affiant was contacted by HSI and was requested to respond to the Peace Bridge. Upon arrival, HSI informed your affiant that CBP had conducted a preliminary border search of ALVAREZ's Samsung Galaxy S9+ cellular telephone, discovering multiple text messages from an unknown individual. These text messages contained addresses and photographs of multiple gas stations, including a gas station that appeared to be in the State of Tennessee. Moreover, HSI informed me that one of the photographs contained on ALVAREZ's Samsung phone was a photograph of gas station security seals, and that according to CBP, the photo appeared to be from approximately 1 year ago. At that time, I inspected the items seized from ALVAREZ's vehicle. In particular, one of the items was a card reader/encoder, which is a device used, along with a computer, to load electronic data onto the magnetic stripe of a card. In addition, I observed 16 internal skimming devices ("skimmers"), and a customized cable, which appears to have been used to connect the computer to the skimming devices. In reviewing all of the credit and debit cards seized, a total of 93 cards were found to be counterfeit, meaning that the account details on the magnetic stripe of the card do not match the embossed information on the card. The account numbers contained on the cards meet the definition of access devices since those account numbers can be used to obtain money, and the re-encoded cards that contain account information meet the definition of counterfeit access devices because they were not issued by the appropriate bank or credit card company. The computer, card encoder, cables and skimmers are device-making equipment since they are all used to create counterfeit access devices. The skimmers are used to collect the account numbers. The cables are used to retrieve the information from the skimmers to the computer. The computer

and the card encoder is used to alter the card's magnetic stripe to become a counterfeit access device.

12. In addition to the counterfeit access devices and manufacturing materials, ALVAREZ possessed 65 gas station security seals, some of which contained Chevron and Sunoco gas station logos. Similar skimming schemes utilize telephonic reconnaissance, similar to the gas station photographs observed on ALVAREZ's phone, to target specific gas station pumps. In order to install an internal skimming device, an individual must destroy the existing security seal to gain access to the gas pump. After the internal skimming device is installed, the individual will replace the destroyed security seal with a counterfeit one, similar to those found in ALVAREZ's possession.

13. In similar skimming schemes, the computer serves as the data storage center for compromised credit and debit card information, as well as the conduit for said information to be transferred onto counterfeit access devices. The computer is often transported directly to the skimming site, so that the compromised data can be quickly uploaded. At the time of his arrest, ALVAREZ possessed a "Cyber Power" 12 volt car charger with a 120V (three prong) output. ALVAREZ's Lenovo Yoga Laptop Computer was the only electronic device found in the vehicle that was compatible with the "Cyber Power" charger, indicating the computer was being used/powered inside the vehicle.

14. Based on my training and experience, I am familiar with fraudulent schemes to obtain money using a skimming device. A skimming device is essentially an electronic device

that captures information contained on a credit or debit card, and can be attached on the face plate of where a card is swiped, or can be placed internally at point of sale terminals more discreetly capture the payment card data. In particular, I am aware of recent fraudulent activity at gas stations, where internal skimming devices are installed to capture the payment card data for cards used purchase gasoline. The information from the skimming device is usually retrieved physically or remotely using Bluetooth or WiFi. At that point, the downloaded information can then be transferred onto blank cards, creating "clones" of the original bankcards.

15. Following the arrest of ALVAREZ, investigation revealed that ALVAREZ booked an airline reservation with Delta Airlines for travel on August 28, 2018, from Los Angeles, CA, to Seattle, WA, and to Anchorage, AK. Additionally, ALVAREZ booked an airline reservation with American Airlines for travel on September 24, 2018, from Denver, CO, to Dallas, TX, and to Memphis, TN. However, during the HSI interview of ALVAREZ on October 11, 2018, ALVAREZ stated that he was self-employed as an air conditioning repair technician, and that he mainly services the Miami, FL area and surrounding suburbs. ALVAREZ also indicated prior travel to Las Vegas, NV, Denver, CO, and Orlando, FL, but did not mention any travel to Washington, Alaska, Texas, and/or Tennessee.

III. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

17. Based on my knowledge, training, and experience, I know that electronic devices, such as the SUBJECT PROPERTY, can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

18. As further described in **Attachment B**, this application seeks permission to locate forensic electronic evidence that establishes how the SUBJECT PROPERTY were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT PROPERTY because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

IV. THE PROPERTY TO BE SEARCHED AND ITEMS TO BE SEIZED

19. Based on the foregoing, there is probable cause to believe that on the SUBJECT PROPERTY, which are more fully described in **Attachment A**, there is located evidence, fruits and/or instrumentalities of the violations specified in this affidavit.

20. Based on the foregoing, there is probable cause to believe that on the above property the items set out in **Attachment B** will be located stored in electronic form.

V. CONCLUSION

21. Based upon the above information, probable cause exists to believe there has been a violation of Title 18, United States Code, Sections 1029(a)(1); 1029(a)(4); and 1344, and that there is probable cause to believe that on the SUBJECT PROPERTY, which are more fully described in **Attachment A**, there is located those items set out in **Attachment B**.

22. In consideration of the foregoing, I respectfully request that this Court issue a search warrant for the SUBJECT PROPERTY, which are more fully described in **Attachment A**, authorizing the search of the aforementioned property for the items described in **Attachment B**.

23. Finally, since this affidavit relates to an ongoing criminal investigation and contains the names of individuals who are witnesses and/or targets in this matter, the government respectfully moves this Court to issue an Order sealing, for 60 days unless the Court orders otherwise, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant.

Michael L. Hamilton, Special Agent
United States Secret Service

Sworn and subscribed to before me
this 23rd day of October 2018.

HON. JEREMIAH J. MCCARTHY
United States Magistrate Judge

ATTACHMENT A
Property to be Searched

The items to be searched are currently in the custody of the United States Secret Service (USSS), and securely located at the USSS office in Buffalo, NY 14202. All of the items to be searched were initially seized by officers with U.S. Customs and Border Protection on October 10, 2018, and were in the possession of JORGE ALBERTO-ALVAREZ. The items to be searched can be further described as follows:

1. One Lenovo Yoga Laptop Computer, 730-13IKB, mode 81CT, bearing serial number MP1DCDQZ, gray in color.

2. One Samsung Galaxy S9+ cellular telephone, with the cellular telephone assigned call number (305) 766-7154, with International Mobile Subscriber Identity/Electronic Serial Number 354645090334800, gray in color.

3. Sixteen skimming devices, the wires gray in color with blue caps and metal pins at the end.

ATTACHMENT B
The Items to be Searched for and Seized

The following items to be searched for and seized on the property listed in Attachment A, whether in physical, documentary, or electronic form, for the period of time of October 2017 to the present, evidencing a scheme to steal credit, debit, and bankcard data using skimming devices and then to encode counterfeit cards with the stolen account information in violation of Title 18, United States Code Sections 1029(a)(1); 1029(a)(4); and 1344, include:

1. Any and all documents, files, records, images, videos, emails, email software, associated email addresses, email address book contents, internet history, browsing history, internet search history, app data, cookies, deleted files, bookmarked and favorite web pages, user typed web addresses, desktop shortcuts, path and file names for files opened through any media and/or image viewing software, peer to peer files, newsgroup postings by the user, and/or IP addresses assigned.

2. Any and all account numbers, routing numbers, credit card numbers, gift card numbers, and other numbers or codes identifying real or fictitious financial accounts.

3. Personal Identification Numbers (PINS) used to obtain access to financial accounts.

4. Personal identifying information such as names, dates of birth, social security numbers, phone numbers.

5. Identification documents, such as drivers licenses, birth certificates, social security cards, passports, resident alien cards, and/or any other type of identification documentation.

6. Records, texts, instant messages, correspondence, emails, photographs and internet history related to online searches for banks, other financial institutions, and/or gas stations where credit, debit, and bankcards can be used.

7. Records, texts, instant messages, correspondence, emails, photographs and internet history related to mapping, location, and direction services.

8. Records, texts, instant messages, correspondence emails, photographs and internet history related to ownership, control, and the identity of users of the searched property.

9. Travel itineraries and receipts relating to flight reservations, hotel lodging, and vehicle rentals.

10. During the course of the search, photographs of the items referenced in Attachment A may also be taken to record the condition thereof and/or the location of items therein.